IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	**)**	
Defendant	**)**	

DEFENDANT'S MOTION FOR DISCOVERY REGARDING GOVERNMENT'S USE OF GOOGLE'S SENSORVAULT DATA

Pursuant to Federal Rule of Criminal Procedure 16 and Mr. Chatrie's constitutional right to due process, Mr. Chatrie requests the following discovery concerning the use of Google's Sensorvault data in this case.

Little is known about how Google collects this location data beyond the media reports cited in Defendant's Motion to Suppress Evidence Obtained from A "Geofence" General Warrant. Even less is known about how the government used the data it obtained or how it purported to "narrow down the list" to determine, at its discretion, which accounts to deanonymize and search additionally. *See* State Warrant at 2[1]. This information is material to preparing a defense for Mr. Chatrie. Thus, Mr. Chatrie requests the following discovery:

1. The location/source of the WiFi/WiFi access points for individuals' location tracking data listed as "WiFi" in the "source" section of Prod01_142 and Prod_163, including all Media Access Control (MAC) addresses, Service Set Identifier (SSID's)

[1] The government has provided the defense with a sealed copy of this search warrant with no explanation as to why it remains sealed. Per the Chesterfield County Circuit Court Clerk's Office, this warrant and its supporting documents will remain sealed absent further intervention from the government until December 19, 2019. Because the document is and will remain sealed until further action by the government, Mr. Chatrie does not attach it here, but refers to it for when the Court is able to review a copy.

information, and MAC addresses for any data that could be associated with a Bluetooth beacon;

2. The anonymous identifier used for Mr. Chatrie's Sensorvault data in this case;

3. Details concerning Google's Sensorvault, including:

    a. how the location data is captured and collected;

    b. how often Google collects location data on Android phones, both through the operating system and through Google applications, services, or software;

    c. how often Google collects location data on non-Android phones using Google applications, services, or software;

    d. all manuals, policies, guidelines, presentations, and protocols relating to how the location data is captured and collected;

    e. all algorithms used in capturing and collecting the location data, including the algorithm version number(s) and year(s) developed;

    f. how Google stores the location data;

    g. all manuals, policies, guidelines, presentations, and protocols relating to how Google stores the data;

    h. all algorithms used in storing the location data, including the algorithm version number(s) and year(s) developed;

    i. how Google analyzes and sorts the location data to respond to law enforcement requests;

    j. all manuals, policies, guidelines, presentations, and protocols relating to how Google analyzes and sorts the location data to respond to law enforcement requests;

k. all algorithms used in analyzing and sorting the location data, including the algorithm version number(s) and year(s) developed;

l. all information about the accuracy of the location data, including any tests, validation studies, error rates and how the error rates were calculated (including whether they reflect test or operational conditions);

4. Parameters of Google's Sensorvault data, including:

   a. how many individuals' tracking information is in the Sensorvault;

   b. how often, if ever, information in the Sensorvault is purged;

   c. who has access to the Sensorvault;

   d. how the Sensorvault is maintained;

   e. all privacy policies relating to the Sensorvault.

5. The name(s) and training, certifications, and qualifications of the individual(s) at Google who gathered and turned over the location data in this case to law enforcement officials;

6. Physical access to any and all devices and software used in this case by any federal, state or local law enforcement official to manipulate and analyze the Sensorvault data;

7. Copies of the raw data produced by Google and utilized by law enforcement;

8. All information about how law enforcement officials manipulated and analyzed the Sensorvault data to identify accounts for which Google provided additional information in the second and third rounds of the search process, including;

   a. how law enforcement officials made determinations about which accounts to investigate further;

b. how law enforcement officials made determinations about which accounts to not investigate further;

c. what data law enforcement officials relied on to make these determinations;

9. Any and all Sensorvault data that Google initially determined to be potentially responsive to the warrant and subsequent law enforcement requests but excluded from the Sensorvault data ultimately Google provided to law enforcement officials in this case, including the reason(s) for the exclusion;

10. The name(s) and training, certifications, and qualifications of the analyst(s) who used the Sensorvault data to identify particular accounts to seek additional information from Google about;

11. For all law enforcement agencies and officers involved in this case, copies of any and all:

a. communications and correspondence between agents involved in the investigation and Google employees/representatives regarding the Sensorvault data in this case;

b. arrest and investigative reports from any officers/analysts who used the Sensorvault data during this case, regardless of whether the Sensorvault data is specifically referenced in the report or not;

c. training materials in the possession of law enforcement agencies for obtaining and using Sensorvault data;

d. contracts, memorandums of understanding and agreements, including but not limited to nondisclosure agreements, concerning the use of Sensorvault data, or that bind the law enforcement agencies;

e. internal policies, guidelines, training manuals, or presentations concerning use of Sensorvault data;

12. All records produced as a result of the requests described above.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2019, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org